DIR
CYBERSECURITY
INSIGHT
Newsletter

March 2014

ADDRESSING THE EVER CHANGING RISKS FOR THE STATE OF TEXAS

Information Security Forum 2014

Thank you for your participation!

Welcome and OCISO Update
Karen Robinson, Chief Information Officer, State of Texas
Brian A. Engle, Chief Information Security Officer, State of Texas

Keynote: Federal Efforts on Cybersecurity, the NIST Cybersecurity Framework, and State and Local Cybersecurity
Andy Ozment, PhD, Senior Director for Cybersecurity, The White House

Intelligence-Driven Security
Michael Brown, Real Admiral , USN (Ret) VP and General Manager, RSA Global Public Sector

Learning From the Mistakes of Others
Jay Jacobs, Senior Data Analyst, Verizon's RISK Team, Verizon

Application Security Threat Modeling
Barry Lyons, Senior Cyber Architect, Northrop Grumman

Advanced Threats Disassembled
Chad Holmes, Chief Security Architect, OCTO, FireEye, Inc.

Adapting Incident Response to Meet the Threat and Minimize the Impact of a Breach
Jeff Schilling, Director, Incident Response and Digital Forensics, Dell SecureWorks

Coming soon - Event Materials

IN THIS ISSUE

The final countdown

Windows XP end of support popup has started. Page 2

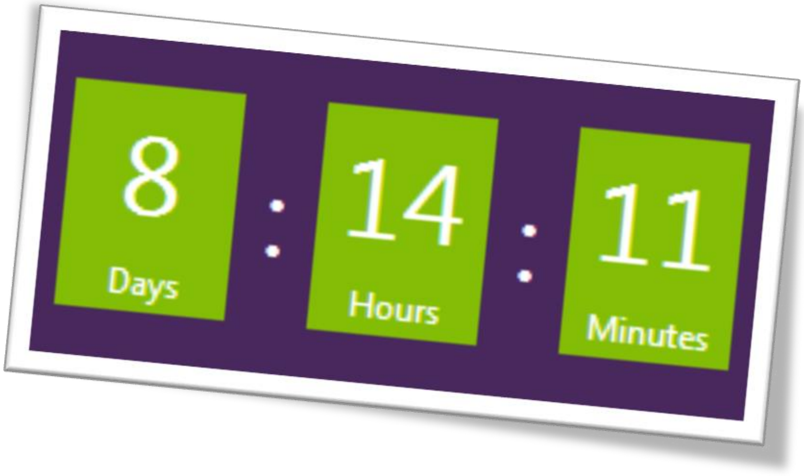
Around the State - ISO spotlight

Meet your peer. Page 3

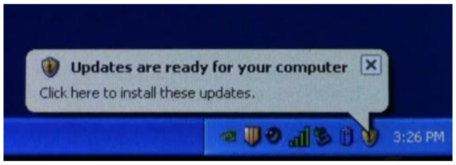
Upcoming Webinars

OCISO is producing a variety of webinars for various roles in your organization. Stay tuned. Page 5

Support for Windows XP ends in:



You won't see any more updates for XP


Updates are ready for your computer

Click here to install these updates.

3:26 PM

Every Windows product has a lifecycle. The lifecycle begins when a product is released and ends when it's no longer supported. End of sale for Windows XP happened in 2008 and Microsoft will end support in 2014. Computers that have XP are at least 6 years old.

Knowing key dates in this lifecycle helps you make informed decisions about when to upgrade or make other changes to your software. Below are the rights and limits of the Windows lifecycle.

End of support

End of support refers to the date when Microsoft no longer provides automatic fixes, updates, or online technical assistance. This is the time to make sure you have the latest available update or service pack installed. Without Microsoft support, **you will no longer receive security updates that can help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information**.

End of sales

End of sales refers to the date when a particular version of Windows is no longer shipped to retailers or Original Equipment Manufacturers (OEM). Examples of OEMs are Dell and Toshiba—PC manufacturers who often preinstall Windows software. When a version of Windows reaches its end of sales date, it's a good time to think about upgrading.

Attacks also happen on computers at home

Who connects to your agency/university network? Are those computers running XP? How are your employees protecting themselves and protecting your agency?

Make sure your VPN connections are also protected with the most recent operating system. Don't let them be the weakest link.

> I drive a 12-year-old Ford, and why not? It's quiet and comfy, and it gets me there.
>
> For many users, XP seems as reliable as my old Ford Taurus. But it's really more like the Ford Pinto, that 1970s car with a bad habit of bursting into flames. And the fire department's about to close. Time to move on.
>
> -Boston Globe

Cost to upgrade your operating system vs the Cost of Risk

After April 8th, IT security risks and compliance issues from continued use will be magnified.

What are the risks?

Technical

- The most common and well-known issue is that patches to mitigate known vulnerabilities will no longer be provided, effectively leaving Windows XP-based systems open to exploits and compromise.
- Newer versions of Internet Explorer, starting with version 9.0, are not supported, meaning that all vulnerabilities in older versions of IE will represent major risks going forward.
- Most peripheral and device vendors will cease to provide new updates patches to their drivers; some have already started subtly doing this. While this represents less of a security issue, this poses sizable compatibility concerns.
- Is well known that many organized hacker groups or organized crime syndicates are developing attacks in anticipation of unpatched Windows XP systems, according to Dark Reading.
- The next generation of malware and virus technologies will be tremendously difficult for Windows XP systems to deal with. One avenue of attack will be a new generation of Advanced Persistent Threats (APT), which are basically targeted attacks focused on a very small number of individual endpoints or users that attackers perceive to be vulnerable.

Legal

- 46 U.S. states have data privacy laws with widely varying non-compliance penalties, each requiring the exercising of due diligence in the protection of private information.

Cost

- The cost of a breach can be substantial.
- Average IT time to handle operational activities (patches, user administration, security activities, maintaining images, etc.) is 3.0 hours per PC for a Windows XP system and only 0.9 hours for Windows 7, based on IDC data. And it doesn't end there. IDC says the average IT hours per PC for downtime totals 2.9 for Windows XP and 0.6 hours for Windows 7.

Are you ready?

SPOTLIGHT

Elaine Mays

Chief Information Officer and Information Security Officer for Texas Juvenile Justice Department.

Tell us about yourself.

I was born in California but spent the majority of my time growing up in Texas. I have several degrees, but the most recent ones are BSBA in Management and MIS (Masters of Science in Management with focus on Information Technology). I have worked with Texas Juvenile Justice Department for one year but have 27 years of state government experience in IT. The majority of my state experience was at TxDPS where I worked in many roles of desktop support, servers, core infrastructure, ITSM, and in management roles. I love to read, so I spend a lot of time reading and with family.

How did you come to the security field?

Being a user and supporting technology automatically puts you in the security field, because it is our duty to ensure that we are taking the necessary steps to secure the integrity and data of our systems. As users we must be mindful of what we access and how we share data, and in the technical role it is our duty to educate our users on how to secure information and ensure that agency systems are secure. In my current role by default I became the interim ISO with no regrets.

What do you like best of your job?

I like serving people (employees, customers, users, etc.). I am a firm believer of "Servant Leadership." I like to drive for results and ensure that the customers receive the best service possible.

TEXAS JUVENILE★JUSTICE DEPARTMENT

Tell us how Information Security has changed since you started in your role.

The one thing I can say that has changed about information security over the years in state government is awareness. We are taking more steps to secure the integrity and data of our systems.

What other career would you have liked to pursue?

I would love to teach leadership because it is a learned trait. I have seen many people become leaders that were never prepared for that position (speaking from experience). Once I acknowledged my lack of skills, then I pursued to be a better leader, and it's a continuous learning process. The other career is computer forensics.

Tell us about your most proud accomplishment?

I've had many proud accomplishments in my career with the assistance of many colleagues, but the most that I am personally proud of is not allowing politics and situations keep me from making decisions that are in the best interest of the agency and the State of Texas.

People would be surprised to know that you…

I was nominated as Female Coach of the Year! I was a certified basketball coach through the Spurs/Pizza Hut league. I was a commissioner in little league baseball and certified coach in Central Texas Pop Warner.

What is the best advice you have received and that you have used?

Continue to learn and grow you. Validate and give accurate information and focus on the things that you can control, and never forget where you come from. Use your past as a growing opportunity for the present and the future. You get out of life what you put into it, and remember the only person that controls your destiny is you! Your response to situations in life is based on how you have allowed the situation to control your reaction.

What would be your advice for a new security professional?

Learn the agency network, know your customers, and maintain the integrity and data of the systems and of yourself. This position requires discipline and being firm on what is the best approach for securing the agency data; however, have an open mind and be willing to listen and communicate with respect! Be willing to look for other ways to implement best practice processes.

http://www.tjjd.texas.gov/

Cybersecurity Tips by

MS-ISAC MULTI-STATE
Information Sharing & Analysis Center

MS

What are Backups?

Backups of computers, laptops, and other devices are important defense layers in recovering from intentional or unintentional loss or corruption of data. For example, critical information can be lost when your hard drive becomes corrupted; natural disasters can destroy your equipment; or malware could infect your computer or device and corrupt your data. With a solid backup and recovery plan, you have a greater chance of recovering from any of these scenarios; without one, those chances are significantly diminished.

Types of Backups

- **Full backup**: A full backup includes all files and software. It is important to consider the amount of storage necessary and the amount of time it would take to not only back up all this information but also to recover.
- **Incremental backup**: In this strategy, a full backup would need to be done periodically, and then only files that have been changed since the last full backup will be replicated. As an example, a full backup may be performed monthly and a differential backup (only the changed information) every day at 5 pm. Differential backups are beneficial in this case because they take less time to conduct, and recovery of information can be more exact to the time the information was compromised or lost.

Backup Storage Options

- **External Drive**: One of the more common methods of backing up information is storing the backup image on a portable drive. This way, if the hard drive on your computer fails, your backup files are still available to restore. To implement this solution an additional device must be purchased and connected to your computer. If the external device is disconnected, your backup will not be performed as scheduled.
- **Cloud-based Backup:** Performing backups to the cloud is becoming more common. Usually this is done via a paid service. Things to consider include cost and location of storage as well as the security controls that the cloud provider has in place. Additionally, be aware that with cloud solutions, backups and recovery speeds depend on the speed of your Internet connection.
- **Hard Drive:** Another common method of backing up information requires the use of an allocated area of the hard drive of your computer. While the process is simple to implement and adds no additional costs, the risk associated with this method is the potential loss of all of your information and also all of your backed up information should you have a serious hard drive failure.

Developing a Backup Plan

Consider the following when developing a plan:

- **How important is the information on your systems or devices?** For critical information, such as contact lists, email, financial transactions, or related business files, you may want to have redundant backup. For less important information, you could back up the information with less frequency.
- **How often does the information change?** The frequency of change can affect your decision on how often the information should be backed up. For example, critical information that changes daily should be backed up daily.
- **How quickly do you need to recover the information?** Time is an important factor in creating a backup plan. For critical information such as business files, you may need to recover your information quickly.
- **Do you have the resources to perform backups?** You must have backup hardware of sufficient capacity and software to perform backups.
- **What is the best time to schedule backups?** Scheduling backups when system use is as low as possible (such as overnight) will speed up the backup process.

Recovery

Backing up data is futile if you cannot recover it. While automated backup strategies are usually efficient, it is a good idea to check on your backup data periodically. This is important not only to make sure that the data is actually backed up and also to review the backup settings.

Gartner Webinar

Why is your organization at greater risk now that is encrypting sensitive data?

Tuesday April 8th, 10:00 AM

Registration at:

[DIR Security Training]

Cybersecurity Online Training

RECORDED WORKSHOPS

Recorded: Insider Threat – Log Analysis & Correlation

In this recorded workshop, you will be introduced to the insider threat *problem* – both malicious and non-malicious. This webinar includes some simple hands-on exercises.

Recorded: Securing Your Wireless Mobile Devices

In this 60-minute workshop, you will be introduced to the different wireless technologies, how they work, and their associated security weaknesses.

Recorded: DoS Wireless Roundtable Discussion

This workshop will sponsor the first roundtable discussion with DoS experts/stakeholders on the state of wireless technology. The discussion will focus on where DoS currently stands and where they are headed.

Recorded: Preparing for an Intl Advanced Persistent Threat

This 60 – 90 minute workshop with demonstration will take a closer look at what Advanced Persistent Threats (APT) are and how they are attacking organizations. This workshop is designed for the beginning to intermediate learner.

Recorded: Network Fundamentals – Part 1

This workshop is part one of a two-part series that will cover network security fundamentals including an overview of network components and how to properly secure your network. Students should have a working knowledge of networking concepts.

Recorded: What your Mobile Device Says About You

Learn to secure your mobile devices with Dr. James Stanger. Dr. Stanger will discuss ways that hackers exploit you, your family, business colleagues, or friends and how you can secure your mobile device to protect you and them from harm.

LIVE WORKSHOPS

Tracking Hackers

Wednesday, March 19, 2014 7:00– 8:00 AM CDT and 12:15 – 1:30 PM CDT

In this workshop, Dr. James Stanger will discuss how to detect, track, and thwart intrusions. He will profile software such as Tripwire, show how to create honeypots, and conduct tracebacks – for learners with a solid knowledge of network concepts.

IPV6 – A Detailed Explanation

Tuesday, March 25, 2014 7:00 – 8:00 AM CDT

This workshop, presented by James Stanger, will present detailed information about how IPv6 works, how it can improve security if properly implemented, and how you can migrate your end user systems from IPv4 to IPv6.

Network Fundamentals – Part 2

Tuesday, April 1, 2014 7:00 – 8:30 AM CDT and 12:00 – 1:00 PM CDT

This workshop is part two of a two-part series that will cover network security fundamentals including an overview of network components and how to properly secure your network. Two 15 minutes hands-on labs will be included.

Insider Threat: User Permissions

Tuesday, April 8, 2014 7:00 – 8:30 AM CDT and 12:00 – 1:30:00 PM CDT

Is your organization prepared for the insider threat? Learn the tools and techniques of the insider threat and how to prepare your organization. Permission escalation and watermarking techniques will be demonstrated with a hands-on lab.

Insider Threat: Securing Privileged Accounts

Thursday, April 17, 2014 7:00 – 8:00:00 AM CDT and 12:00 – 1:00:00 PM CDT

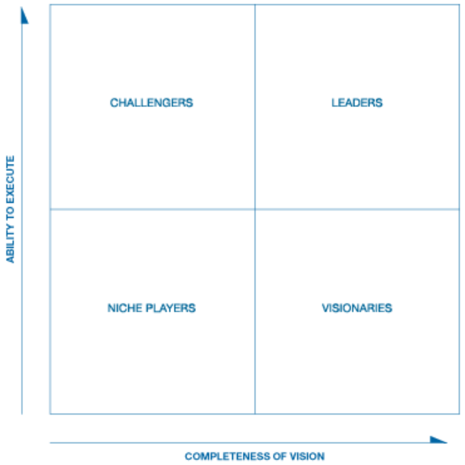
This workshop focuses on proper use and safeguards for Active Directory administrator accounts and Managed Service accounts at Department of State. This workshop is designed for Microsoft Active Directory accounts with elevated levels of access.

Security Services

Decision Support – Gartner Research Access.

Have you recently used the quadrants at Gartner Research?

Who are the competing players in the major technology markets? How are they positioned to help you over the long haul?



Have you talked to a Gartner analyst?

Analysts can drive through the different options for your next project

Do you have your access license? Did you know that all state Agencies and higher education ISOs are entitled to have one?

For more information on Security services, email Office of the CISO.

DIR CYBERSECURITY INSIGHT
Newsletter

DIRsecurity@dir.texas.gov

Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas